

## BUG BYTES JULY 2024



52,429

VULNERABILITIES SINCE LAUNCH

6,369

RESEARCHERS SINCE LAUNCH

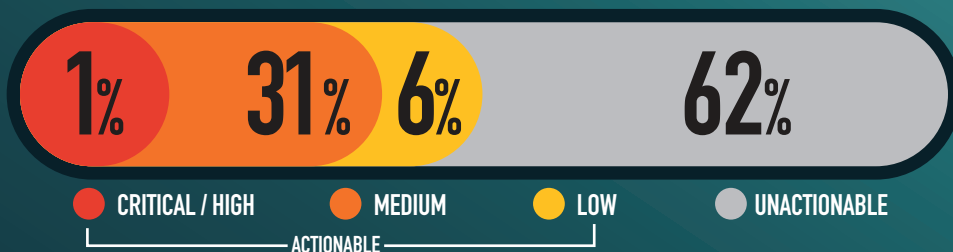
29,006

ACTIONABLE REPORTS PROCESSED

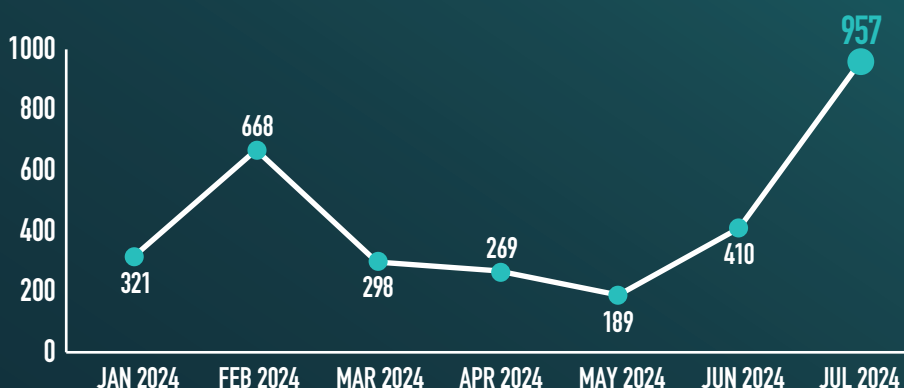
365

ACTIONABLE VDPs FOR THE MONTH

## SEVERITY FOR THE MONTH



## SUBMITTED VULNERABILITIES



## LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH



## KNOWLEDGE BYTE

In July 2024, the DoD VDP received a critical severity submission utilizing insecure credential storage and session prediction vulnerabilities to gain unauthorized access to custom web applications. Researchers identified hard-coded security keys within the application source code that would aid in generating custom access tokens. The custom tokens, combined with predictable session creation logic in the application, could have potentially led to the takeover of privileged accounts on the platform. System owners are encouraged to audit applications to ensure sensitive credentials are properly restricted regularly.

Further information is available in the following resources: [https://cheatsheetseries.owasp.org/cheatsheets/Secrets\\_Management\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Secrets_Management_Cheat_Sheet.html) & [https://owasp.org/www-community/attacks/Session\\_Prediction](https://owasp.org/www-community/attacks/Session_Prediction) & [https://rohan.padhye.org/files/key\\_leaks-msr15.pdf](https://rohan.padhye.org/files/key_leaks-msr15.pdf)

## RESEARCHER OF THE MONTH

**Cybersecurity Spotlight!** A big thank you to [@mikel-22](#) for uncovering a critical session fixation vulnerability (CWE-384) in DOD's Catapult. His diligent work helps safeguard our systems from potential breaches.

**Action Item:** Eliminate hardcoded tokens from source code. #InfoSec #CyberSecurity #DOD